Upholding information rights

45 Melville Street, Edinburgh, EH3 7HL
T. 0303 123 1115 E. scotland@ico.org.uk
www.ico.org.uk

The Information Commissioner's Office response to the Scottish Government's consultation on Improving Multi-Agency Risk Assessment and interventions for victims of domestic abuse

Introduction

1. The Information Commissioner's Office (ICO) is pleased to respond to the Scottish Government's consultation on Improving Multi-Agency Risk Assessment and interventions for victims of domestic abuse.

2. The ICO has responsibility for, amongst other things, promoting and enforcing the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (DPA 2018).

3. The ICO is independent of government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO does this by providing guidance to individuals and organisations, solving problems where we can, and taking appropriate action where the law is broken.

4. Data protection legislation protects individuals' personal data rights. When personal data is lost, stolen or shared or used inappropriately it can lead to harm, distress and negative impacts on personal rights and freedoms. Strong personal data protection policies and procedures should be a central feature of multi-agency interventions for victims of domestic abuse so as to minimise the risk of additional harms or distress to vulnerable individuals and families.

5. In our response to this consultation we first set out some general points about the requirement to consult with the ICO, joint data controllership and data protection impact assessments. We then go on to provide answers to the consultation questions relevant to our role and where we have relevant insight and information.

Consultation with the ICO

6. Article 36(4) of the GDPR requires the Scottish Government to consult with the ICO when developing proposals for legislation to be passed by the Scottish Parliament, or regulatory measures based on such legislation, relating to the processing of personal data This includes:

i. primary and secondary legislation;
ii. regulatory measures (such as regulations, directions and orders) made under primary or secondary legislation;
iii. statutory codes of practice; and
iv. statutory guidance.

7. Consultation is directly with the ICO and is separate from any public consultation, which would not satisfy the above requirements. Consultation should be undertaken during the formative stages of the development of policy, to ensure that there is the opportunity to give due consideration to input from the ICO before the outputs are finalised.

8. We look forward to the Scottish Government undertaking detailed consultation with us as its proposals develop.

Data Controllership

9. The Scottish Government should consider whether the agencies involved in the sharing and processing of personal data as part of a multi-agency assessment and intervention are joint controllers under the GDPR. This would be the case where the partners have joint responsibility for determining the purpose of and means of personal data processing as part of the multi-agency assessment or intervention.

10. Joint controllers must have a transparent arrangement about their roles and responsibilities for complying with the GDPR and are jointly responsible for the data processed as part of the multi-agency assessment and both the ICO and individuals may take action against any agency regarding a breach of those obligations.

11. In situations where there is joint controllership, a single point of contact often makes it easier for individuals (including, in this case, vulnerable individuals and their children who are the subject of multi-agency assessments or interventions) to exercise their rights. We therefore recommend that joint controllers arrange between themselves who will take primary responsibility for complying with GDPR obligations, in particular transparency obligations and individuals' rights, and make this information available to individuals.

12. The ICO is currently drafting a Data Sharing Code of Practice as required under s121 of the DPA 2018. It is anticipated that the Code will be laid

before the Westminster Parliament in Summer 2019. When published, the data controllers should ensure that their processes follow the good practices outlined within it.

Data Protection Impact Assessment

13. A Data Protection Impact Assessment (DPIA) is a process that helps data controllers identify and minimise the data protection risks of a project or processing operation. Article 35 (1) of the GDPR sets out that: "*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purpose of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*."

14. Multi-agency risk assessment will, by its very nature, involve the sharing (processing) of highly sensitive personal data (including what the GDPR refers to as 'special category' data) which, if lost, stolen, disclosed or used inappropriately could lead to a high risk to the rights and freedoms of the individuals involved.

15. While Multi-Agency Risk Assessment Conferences (MARACs) have been operating for a while in some parts of Scotland, the improvement process is an opportunity to clarify roles and responsibilities, to identify ongoing issues and risks, to identify improvements and mitigating actions and to ensure Scotland wide consistency.

16. Undertaking a DPIA will aid the improvement process by providing clarity, on amongst other things: what kind of personal data is shared and why; what happens to personal data after it has been shared; whether sharing and further processing is necessary, proportionate and lawful and help the agencies involved identify less risky ways to use and share this personal data whilst still fulfilling the objectives of the multi-agency assessment process to keep victims safe.

17. Completing a DPIA will also assist the agencies involved in multi-agency interventions with their obligations under the GDPR and DPA 2018 to be transparent about the personal data they process and how they protect that personal data.

18. The ICO therefore recommends that:

- The Scottish Government carry out a DPIA on policy proposals arising from this consultation. A DPIA will help ensure that proposals improve outcomes for victims of domestic abuse and their families whilst also protecting their personal data rights (and those of the perpetrator). A DPIA will also help identify appropriate accompanying national measures, guidance and protocols.

- Relevant agencies carry out a DPIAs on local multi-agency assessment and intervention arrangements. Local DPIAs will assist agencies in identifying appropriate local measures to take to minimise risks to the rights and freedoms of individuals these will include local data sharing agreements.

19. Should the DPIA identify a high risk that the partners cannot mitigate, the relevant agencies should consult with the ICO in relation to the proposed processing (Article 36 (1) of the GDPR).

Our response to the consultation questions

Question 1: How can we ensure training on domestic abuse and appropriate risk assessment tools for public bodies, agencies and services staff?

20. The GDPR and DPA 2018 require that data controllers implement appropriate technical and organisational measures to ensure compliant processing of personal data. It is our view that such measures should include regular data protection training and awareness raising so that staff involved in information sharing are best able to uphold individual's data protection rights. Failure to do so may lead to regulatory action being taken against the data controller

Question 4: In your view, who are the key partners that should be involved in multi-agency working to support victims of domestic abuse?

21. The ICO has no view on which partners should be involved. Whether the agency involved is a public body or a third or private sector body however, may have a bearing on the lawful basis and indeed the lawfulness of certain types of data sharing (see our answers to Question 6 and 7 below).

Question 5: In your view, what guidance is required to support and embed effective multi-agency working for victims of domestic abuse?

22. National guidance should include specific guidance on the protection of personal data shared during multi-agency interventions (see our response to Question 6 below for more detail). Any guidance should be informed by the DPIA.

23. If the Scottish Government produces any statutory guidance relating to the sharing of personal data within the MARAC scheme, it must consult the ICO during the development of that guidance. All guidance relating to data-sharing should ultimately be made compliant with the forthcoming ICO Code of Practice on Data Sharing.

Question 6: What protocols need to be put in place to ensure effective information sharing between agencies?

24. To protect personal data rights, the ICO recommends that the Scottish Government develop a high-level national data sharing protocol (informed by a DPIA). This protocol can provide a framework for more detailed local data sharing agreements between the local agencies involved. These protocols should be based upon the ICO Code of Practice on Data Sharing.

25. Key data protection considerations when developing a national data sharing protocol will include:

26. Lawful basis:

- Personal data must be processed in a lawful, fair and transparent manner. This means, that processing must have a lawful basis as set out under Article 6 of the GDPR. If the data in question includes 'special category' data a condition under Article 9 of the GDPR must also be met for processing to be lawful.

- If the data relates to criminal convictions or offences then additional safeguards must be in place and under Article 10 of the GDPR it can only be shared if UK law permits. The DPA 2018 sets out the relevant UK law covering this type of processing in Schedule 1.

- The lawful basis for sharing personal data relating to multiple parties (the victim, the perpetrator, other family members) should be

established on a case by case basis according to the type of personal data, who it relates to and the purpose for sharing.

- MARAC guidance produced by Safelives suggests that it is good practice to seek consent from individuals to share information at a MARAC. Under previous data protection legislation this consent may have been sufficient for lawful processing. The GDPR however, sets a high standard for consent. A controller must be able to demonstrate for example, that a victim's consent is freely given. This may be difficult to demonstrate where power imbalances exist e.g. between victims and the police or other professionals. Existing consent mechanisms should therefore be reviewed to ensure that they meet the GDPR standards.

- As part of the improvement process the Scottish Government and partner agencies may determine that in some contexts where consent has been relied on in the past another lawful basis for processing personal data in multi-agency assessment or intervention settings may now be more appropriate. If information sharing is likely to take place whether the victim gives consent or not, then another legal basis should be relied upon.

- Where the police share information collected for law enforcement purposes with other agencies for non- law enforcement purposes particular care should be taken. See our response to Question 7 below.

27. Transparency:

- Whichever legal basis is relied upon agencies must comply with the transparency requirements of the GDPR. The DPIA can assist with this.

- Transparency obligations vary according to whether data was obtained from the individual directly or via third party. Multi-agency assessments and interventions will involve data obtained both from the individual involved and from third parties (relating to, for example, the perpetrator or other family members). Article 13 of the GDPR sets out what information individuals should be provided with where data has been obtained directly from them, and Article 14, where it has not.

- This 'privacy information' includes details of what kind of personal data is being processed, the purposes of processing and which organisations or bodies that information is being shared with.

- These requirements, could, in certain circumstances, prejudice the multi-agency assessment process. There are exemptions available that may be relied on in these cases. Article 14 (5) (b) for example, sets out that the requirements do not apply when the provision of this information to the individual is likely to 'render impossible or seriously impair the achievement of the objectives of that processing'. Schedules 2, 3 and 4 of the DPA 2018 contain further exemptions which can be considered on a case-by-case basis.

- There is a specific exemption from Article 15 requirements (confirmation of processing and the right of access) when a serious harm test is met i.e. where the application of Article 15 rights would be likely to prejudice carrying out social work because it would be likely to cause serious harm to the physical or mental health of the data subject or another individual.

28. Data minimisation:

- Article 5(1)(c) of the GDPR sets out the principle that data processing should be adequate, relevant and limited to what is necessary. This means that participating agencies must ensure that they share only that personal data which is necessary to safeguard and support victims and also that all relevant personal data that is necessary to achieve that purpose is shared. Case by case judgement will be required to balance the rights and freedoms of the individuals at risk with the data protection rights of those individuals and others. The local data sharing agreements should detail which data sets will be shared and with whom.

29. Storage limitation:

- Article 5(1)(e) of the GDPR sets out that personal data should only be kept in a form that permits identification of the subjects for as long as necessary. The factors that determine appropriate retention periods will vary according to the type of data and circumstances. Data sharing protocols should set out in more detail the factors that determine how long this should be. The Scottish Government could set them out in legislation. Local data sharing agreements should set out a procedure for dealing with cases where different organisations have different statutory or professional retention periods as well as common rules for retention.

30. Integrity and confidentiality:

- Article 5(1)(f) of the GDPR sets out that personal data should be processed in a manner that ensures appropriate security against unlawful or unauthorised processing, accidental loss, destruction or damage.

- Local data sharing agreements should set out how this will be achieved and include detail about technical and organisational arrangements for secure transmission of the data and procedures for dealing with a data breach. Getting the basics right is, in this context, as important as the technical fixes1.

- A personal data breach is a a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Personal data breaches which are likely to result in a risk to individuals rights and freedoms must be reported to the ICO within 72 hours of establishing that the breach has taken place and where there is a high risk of adverse impact on the rights and freedoms of those effected.

- Local data sharing agreements should set out the procedures for detecting, investigating, managing and reporting breaches of personal data shared by multi-agency partners. The procedure should set out the process for informing multi-agency partners and effected individuals.

- The requirement to communicate a personal data breach could in some circumstances place the multi-agency intervention at risk. For example, if it means informing third parties (such as the perpetrator) that they are being discussed.

- Schedule 2 of the DPA 2018 sets out exemptions to Article 34 (1) and (4) of the GDPR (the requirement to communicate a personal data breach to effected individuals). Schedule 2 Part 1 provides an exemption where personal data is being processed for the prevention or detection of a crime.

31. Data protection and personal data rights:

[1] For example, in June 2018 the ICO took action against Gloucestershire Police for revealing identities of abuse victims in bulk email. In this particular case the full names and personal email addresses of individuals who were or were associated with victims of child abuse were revealed to over 50 recipients of a bulk email because the sender failed to use the 'Bcc' field

- Data sharing protocols should set out clearly the personal data rights of the victim, their family and the perpetrator and how these will be upheld. The obligation to uphold these rights applies to each of the agencies processing shared data.

- If it is determined that the agencies involved in the multi-agency intervention arrangements are joint controllers then consideration should be given to how best to facilitate individuals in exercising their data rights. This may involve identifying a coordinator to take overall responsibility.

32. Children:

- The GDPR states that "children merit specific protection with regard to their personal data".

- This means that where multi-agency assessments or interventions share personal data relating to children specific care should be taken to ensure that the privacy information provided to the children involved is clear, in plain language and understandable to the child.

- Where data sharing about a child is based on consent the agencies involved will need to consider the competence of the child (whether they have the capacity to understand the implications of the processing of their personal data). If it is determined that the child has the capacity to give consent then they are considered competent to give their own consent to the processing, unless it is evident that they are acting against their own best interests.

- Section 208 of the DPA 2018 states that children in Scotland can give consent where the person is taken to have the capacity to have a general understanding of what it means to give such consent and that a person aged 12 or over is presumed to be of sufficient age and maturity to have such an understanding unless the contrary is shown.

- Agencies should however take into account any imbalance of power in their relationship with the child, to ensure that consent is freely given. See our advice above which stresses the need to be cautious about using consent as a lawful basis in situations where there is an imbalance of power and/ or information would be shared in the absence of consent.

33. Accountability:

- Each agency must be responsible for and be able to demonstrate compliance with the six data protection principles set out in Article 5(1). A DPIA, the national data sharing protocol (high-level framework) and the local data sharing agreements (setting out the detail of what this looks like in practice at the local level) will aid the agencies involved in demonstrating accountability.

34. Dissolution:

- Data sharing protocols and local data sharing agreements should set out a clear procedure for when the local data sharing arrangement is dissolved and what should happen to any shared data held by partner organisations.

Question 7: Do you think that multi-agency arrangements for protecting victims of domestic abuse should be placed on a statutory footing?

35. Following this consultation, should the Scottish Government determine that Police Scotland should be a partner in multi-agency assessments and interventions then the Scottish Government should be aware of section 36(4) of the DPA 2018 that states that 'personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law'.

36. Law enforcement purposes are defined in the DPA as the: 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties including safeguarding against and prevention of threats to public security'

37. Section 36(4) may therefore prevent the police disclosing information collected for law enforcement purposes to the other agencies without it being authorised by statute, statutory Code of Practice, common law or Royal prerogative.

38. Some disclosures of personal data collected as part of a criminal investigation may be authorised by legislation such as the Adult Support and Protection (Scotland) Act 2007 but providing multi-agency assessments or interventions for victims of domestic abuse with a statutory basis may provide a clearer lawful basis and allow for a less restricted flow of information.

39. The Scottish Government should satisfy itself that there is a clear legislative basis for multi-agency information sharing involving personal data collected for law enforcement purposes. Further ICO guidance on the above issues will be forthcoming.

We trust this response is helpful. Should the Scottish Government require clarification of any of the points made, please contact us on 0303 123 1115 or by email at scotland@ico.org.uk.